Synopsis

On

Enhance Smart Cities Security by Mitigating IoT Vulnerabilities

Research Proposal Submitted for Partial Fulfillment of the Requirements for the Degree of

DOCTOR OF PHILOSOPHY

B

Bhupendra Singh Dhakrey

Under the Supervision of
Dr. Hari Om Sharan

Submitted to

Department of Computer Science & Engineering

Faculty of Engineering & Technology

Rama University Uttar Pradesh Kanpur

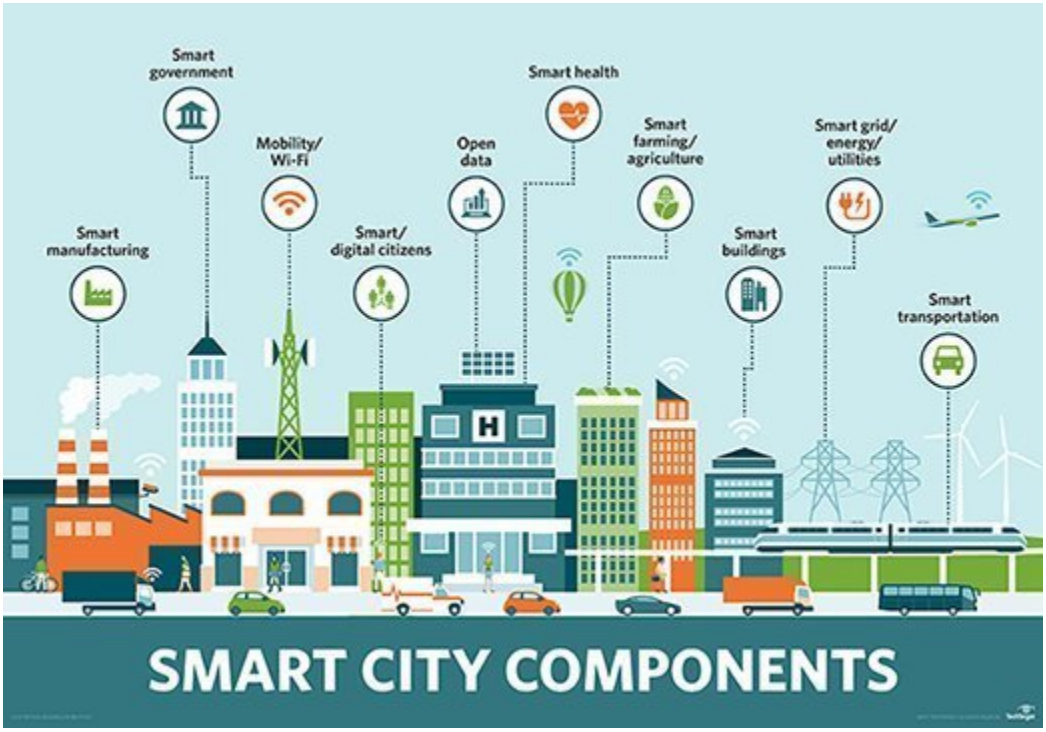
Rama City, Mandhana Kanpur (U.P.) 245 304

Table of Contents

Enhance Smart Cities Security by Mitigating IoT Vulnerabilities 1
Introduction 3
Literature Review 15
Objective 17
Research Methodology 18
References 21
Plagiarism Checker Report 22

Introduction

A Smart city[1]is a municipality or urban area that use large amount and different type of sensors to collect and process data to analyze, manage and monitor information about different systems like traffic, power plants, school, library, transport, waste, law enforcement and other community services.



Smart city uses information and communication technology to enhance service quality, performance, economic growth, clean and sustainable environment to reduce cost, waste and consumption. The Information and Communication Technology (ICT) and Internet of Things (IoT) integration provide us efficiency of services, operations and connect of citizen.

Smart cities deal in large volume of real time data. Smart Cities have many resources which produces different type of data. It's necessary to maintain the privacy of public and personal data hence smart cities security is very important

issue that can affect data and privacy issues like Theft, Eavesdropping, Denial of Service (DoS), Phishing, Spoofing Attacks on Data integrity, Identification and Secondaryuse. Personal data can be sensitive or non-sensitive. The non-sensitive data can be transmitted without encryption and itwon't harm to person which it belongs to however if sensitive data/information passed without encryption it could harm the person it belongs to. This information is Biometric, Medical, Financial, passport, PAN,UIDAI Aadhaarnumber or any other personal information[2].

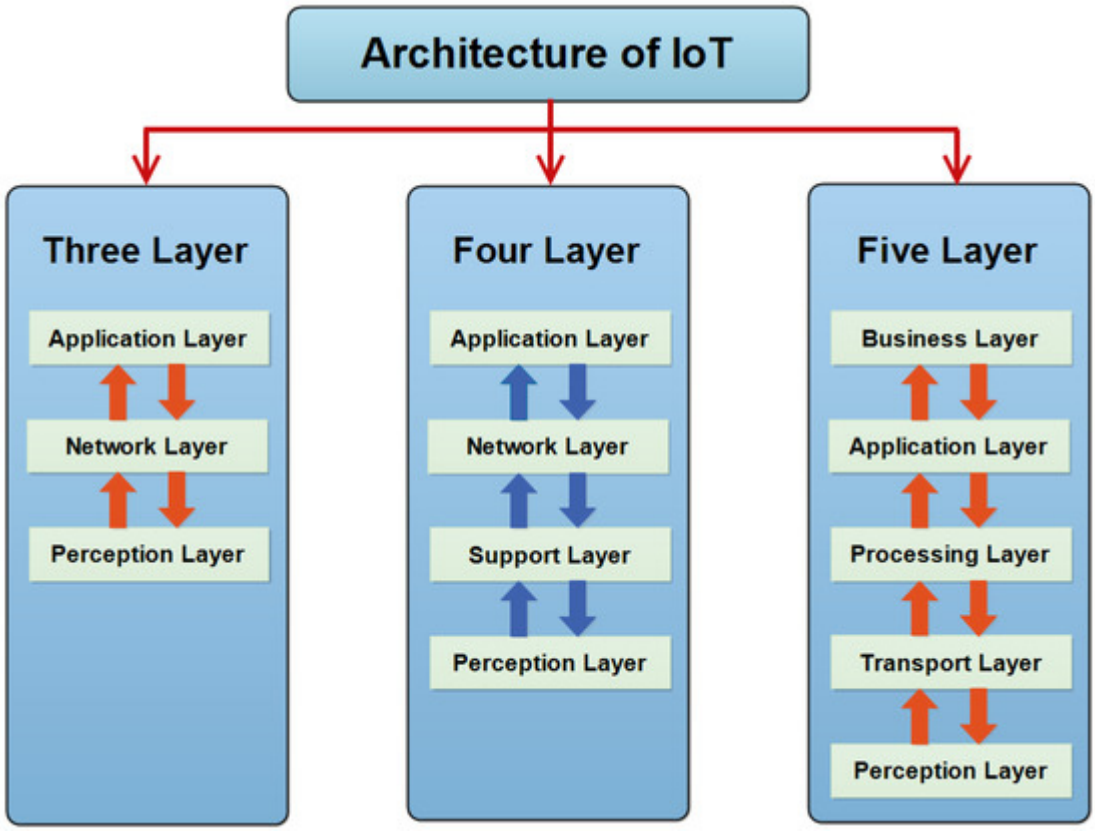
Smart city challenges and concerns:

The key objective is smart city to collaborate public, private and city resident to create smart citizen. Expectations from smart citizen isthat they will positively contribute to community and city.

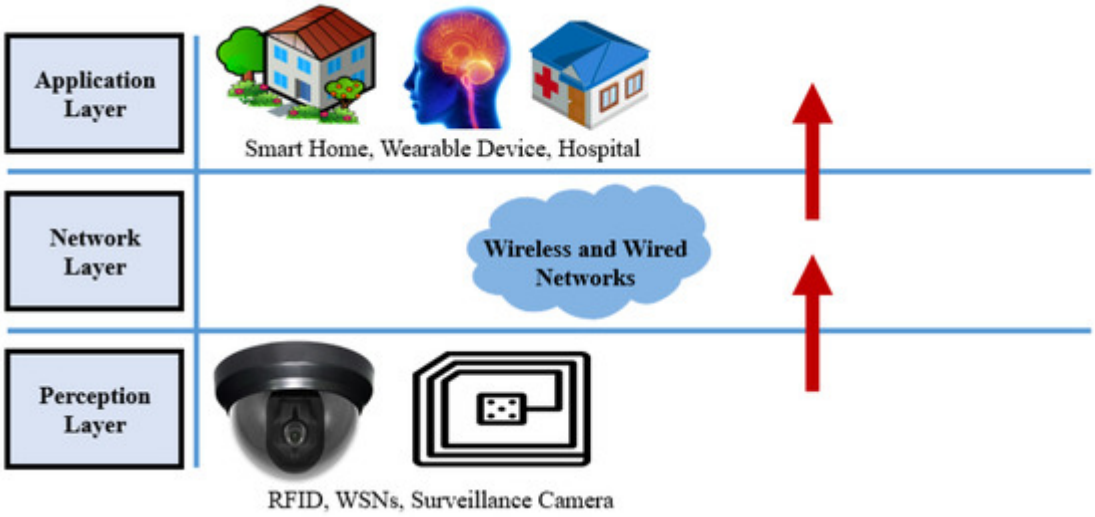
Smart City to ensure data is available to users to allow them to complete use the same for paying bills, use transport and see water, electricity consumption.

Data privacy and security are top most concerns. The presence of sensors and cameras may perceive government surveillance. Data collected should be anonymized and it should not be PII (Personally Identifiable Information)[3]

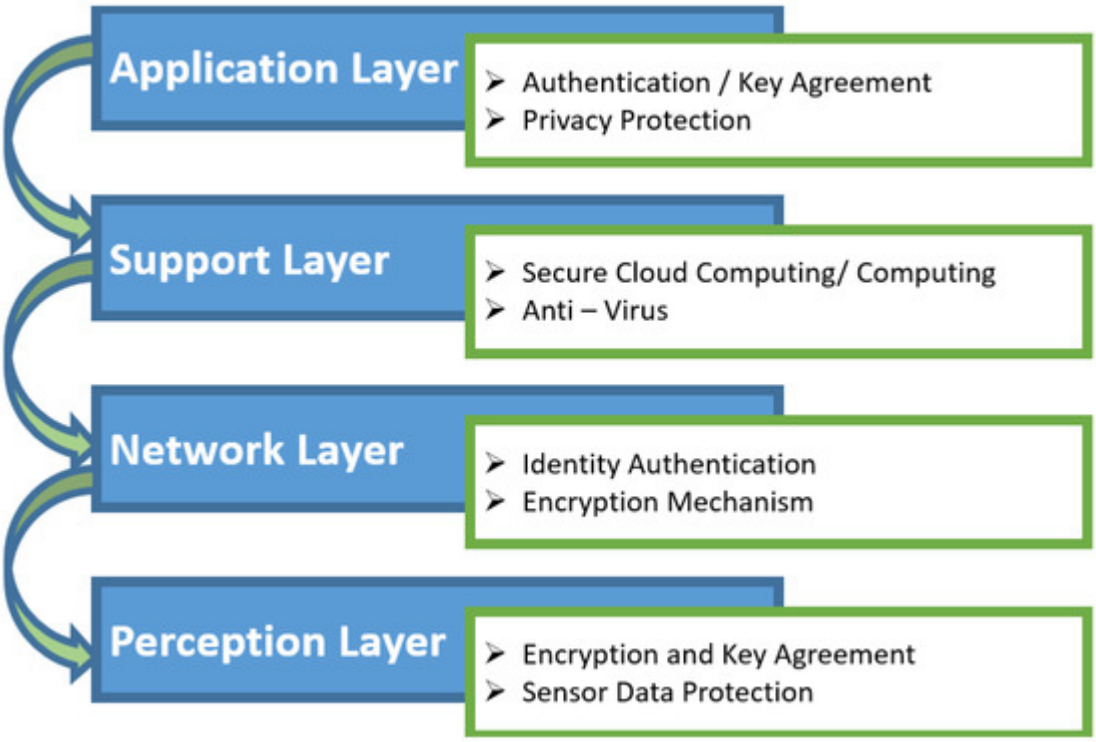
There is no uniform architecture for smart city however we can divide smart city architecture in below mentioned layers [4]

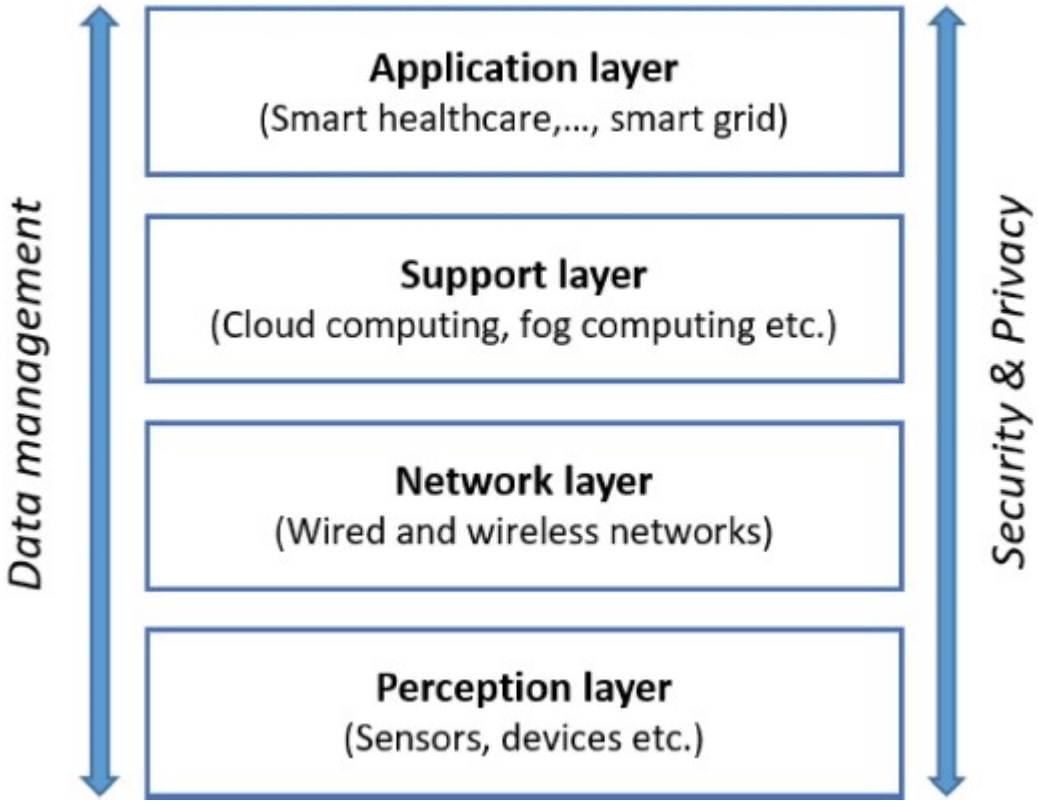


Three Layer Architecture[4]



Four layeredarchitectsare most commonly used[4],[5].





Application Layer: It's top layer and it provide services related to monitoring and other services to user based on personalization requirements.

Support Layer: This layer help application layer in computing like cloud, fog and edge computing.

Network Layer: This layer is core layer and responsible for data transmission, collected by Perception layer.

Perception Layer: This layer is lowest layer and known as edge layer or sensing layer. This layer mainly used to collect data from things and transmitting data to Network layer for further processing.

Business Layer: The Business Layer responsible for management and control of the applications. This layer is also responsible for user privacy management.

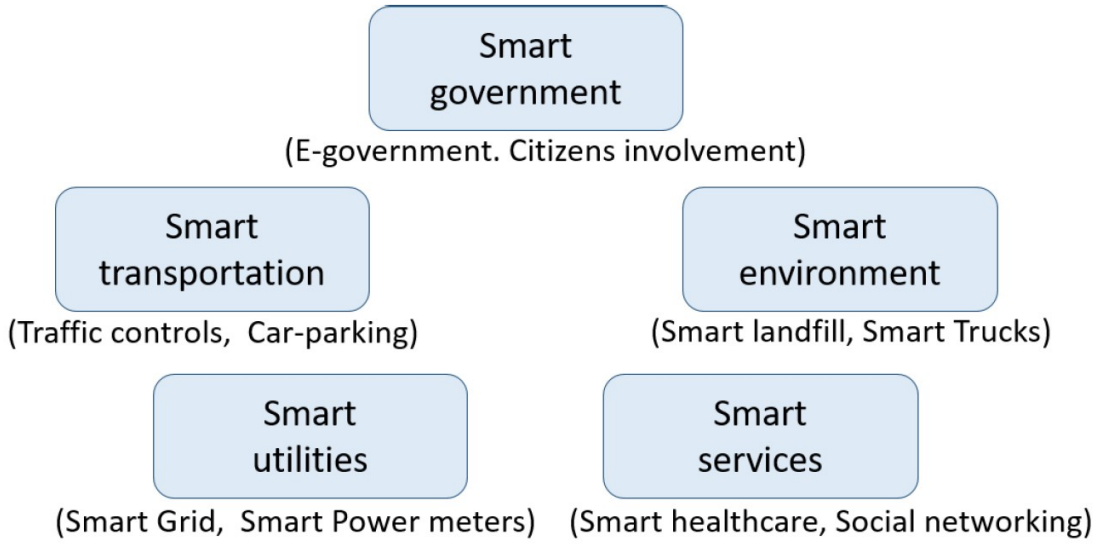
The major problems with business layer security are

1. Business Logic Attack: This may result due to common flows in the business layer due improper coding, validations and encryption techniques.

2. Zero-Day Attack: This problem in application happens when we have security hole or application issue which is not known users and attacker take control withoutuser consent.

Smart City Applications:

The one of the main objectives of developing smart cities to benefit citizens by offering then different aspects like environment,energy, services and industries. We have below main applications in Smart Cities.[5]



Smart Government:
The key purpose of smart government to serve its citizen with infrastructure, data, involve them in key decisions, planning and raise grievance. It's crucial application in smart city.

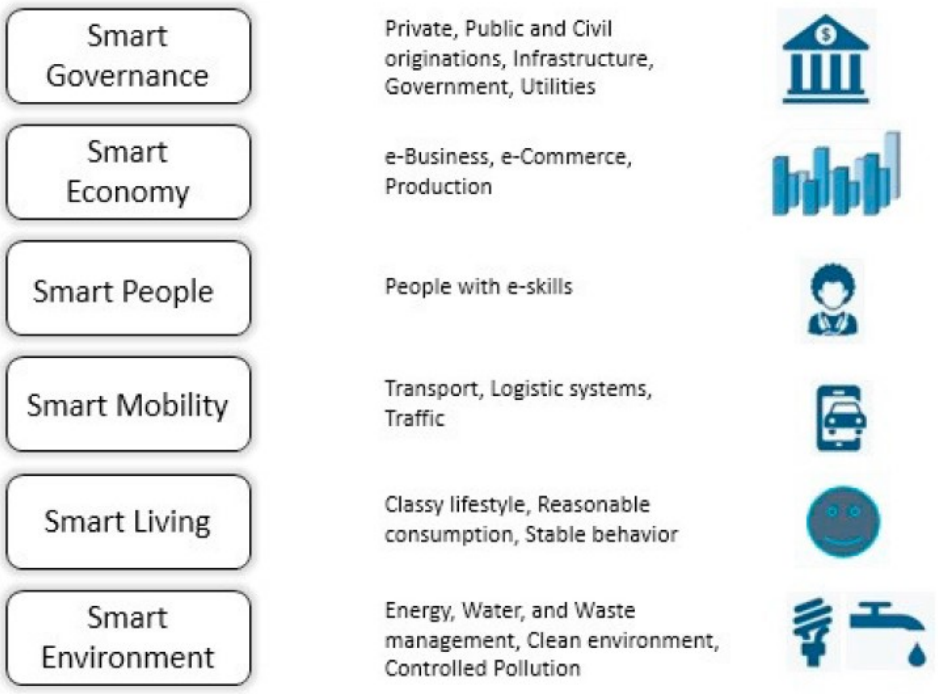
Smart Transportation:
This application helps in finding transportation facility, identify fast routes, vehicle parking search and driving license issue.

Smart Utilities:
This application helps in reducing waste, water, light, gas and thus help in protecting environment.

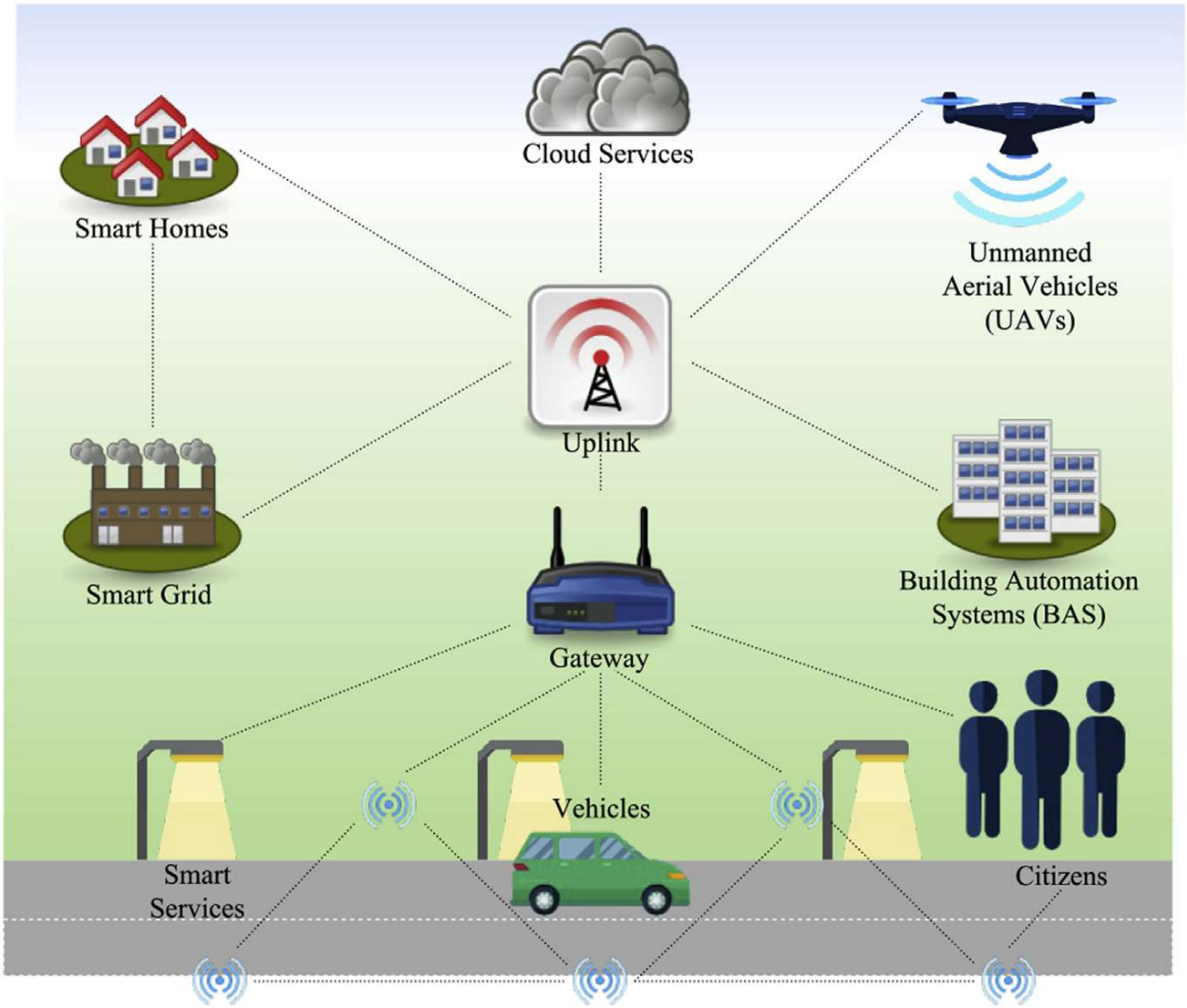
Smart Service:
This application provides medical facility to citizen, monitor health parameters, social networking and comfortable living environment.

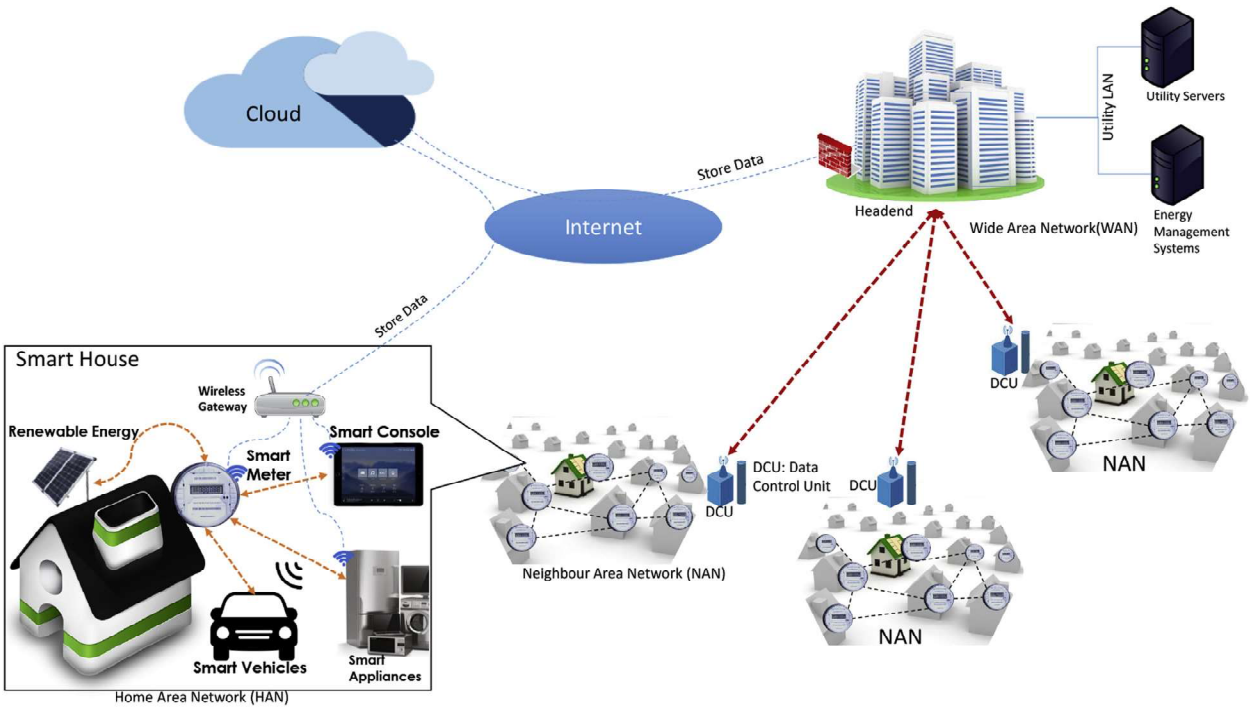
Smart Environment:
This application helps in monitoring air quality, waste management efficiency, predict natural disaster and energy consumption.

Few more applications [7]



Interconnected smart city components[8]




Cloud
Internet
Store Data
Store Data
Headend
Utility LAN
Utility Servers
Energy Management Systems
Wide Area Network(WAN)
Smart House
Wireless Gateway
Renewable Energy
Smart Meter
Smart Console
Smart Vehicles
Smart Appliances
Home Area Network (HAN)
Neighbour Area Network (NAN)
DCU
DCU: Data Control Unit
DCU
DCU
NAN
NAN

Current Security and Privacy Protection Technologies

Disciplines	Year	References	Applications scenario	Technologies
Cryptography	2017	[35]	Smart transportation	Two-level authentication key exchange scheme
	2016	[36]	Smart grid	Homomorphic encryption
	2017	[37]	Smart shopping	RFID
	2016	[38]	Smart card	Zero-knowledge proofs
Blockchain	2017	[39]	Smart home	Blockchain-based smart home architecture
	2017	[40]	Smart transportation	Network topology and decentralized blockchain-based framework
	2017	[49]	IoT architecture	Distributed architecture based on blockchain technique and fog computing
Biometrics	2016	[41]	Mobile sensors	Cascading bandpass filter for noise cancellation
	2017	[51]	Storage devices	Biometric based authentication and key negotiation protocol
ML and DM	2017	[56]	Wi-Fi networks	Deep feature learning
	2015	[57]	Smartphone	SVM-based authentication system
	2017	[58]	Mobile devices	Bayesian linear regression model
	2017	[64]	Social networking	Privacy preserving k-means clustering
Game theory	2017	[68]	Low-resource IoT devices	Nash Equilibrium
	2016	[69]	Honeypot-enabled networks	Bayesian game of incomplete information
	2016	[71]	Wireless networks	Zero-sum game
Ontology	2016	[77]	Smart home	Layered cloud architectural mode based on ontology
	2017	[79]	Mobile computing	Context-aware and personalized privacy control
	2017	[82]	IoT architecture	Semantic-ontology-based situation reasoning method

We have above current technologies for handling data and privacy security threats[5].

Key privacy related challenges and violations [7]

Table 1.Privacy-related challenges and violations

Category	Privacy-Related Challenge	Violations	Description
Communication Privacy	• M2M communication • Citizen to smart city communication	Eavesdropping	To spy on all kinds of conversations and recordings and to listen to communication channels; or we may say reading data by unauthorized readers[17].
		DOS	To block all system's operations by using its radio signals for broadcasting devices for malicious purposes; or we may say to blind smart cities[18].
		Man-in-the-Middle attack	Intercept communication channels to manipulate transmitted data, and falsified operators' actions [16]
		Side Channel Attacks	To use whatever reached information about the physical implementation of computing tasks such as power consumption and execution time [19, 20]
		Identification	Linking data and information to whom they belong.
		Secondary use	Using data and information collected according to specific permission and particular use for another unpermitted purposes.
Business Privacy	• Banking • E-commerce	Phishing	To impersonate trusted reputable party for gaining critical information such as passwords and credit cards n40bers via emails and instant messages [21].
		Spoofing	To duplicate data by third malicious and send it to the reader after revealing the security protocol[16].
		Attacks to data integrity	Get information about customers and networks and inject false data to system's monitoring centre[22].

Summary of the smart city security and forensic data landscape.

	Security threats	Data sources	Forensic data (Level of requirement)	Challenges
Smart Grids	• Protocol vulnerabilities • Privacy • Eavesdropping • Rogue/infected devices • Attacks on internet connected devices	• Communication gateways • Smart meters • ICS systems • Smart Appliances • Sensors/Actuators • Firewall • IDS/IPS	• Connection logs (syslog, console logs, network packet capture): High • Usage logs: Medium • System logs (authentication, OS, application): High	• Large Data Volume for analysis • Data Privacy • Preservation costs
BAS	• Highly Trusting devices • Long device lifecycle • Lack of source authentication • Insecure protocols	• Internal Logger devices • Firewall/IDS (if implemented)	• Trend logs (value changes): High • Connection Logs: High • CSV: High • Other DB format: Variable • SQL: High	• Reliance on thorough device logging; not all I/O are logged automatically. • Extraction of complete logs. (Log buffers are volatile)
UAVs	• Communication interception • Communication injection • Communication jamming	• Drone • Cloud management system • Controller	• Flight logs: High • Connection logs: High • System logs: High • Flight videos: Medium • GPS data (drone and controller): Medium	• Extraction of live drone state without power down
Smart vehicles	• Physical threat • Communication interception • Communication jamming/DoS • Data security	• GPS • Infotainment system • Event data recorder	• Connected device logs: High • System logs: High • GPS data: High	• Validity of retrieved log data • Authorized access to vehicle data
IoT sensors	• Maintaining confidentiality of data • Secure communication • Data management • Data storage • Sensor failure • Remote exploitation	• Smart parking meters • Structural health measurement devices • Smartphone detection sensors • Electromagnetic field level monitors • Traffic congestion monitors • Smart lighting sensors • Waste management monitors • Smart roads sensors	• Serial numbers of sensor, location, temperature, humidity, timestamp High • Log files in .log or .csv format: High • Data can be stored in .csv or .log format: High	• Sensor data compromise (integrity). • Data security on transmission line. • Authorized ac- cess to sensor data.
Cloud	• Data Leakage • Malicious insider threat • Insecure API • Denial of service (DoS) • Malware injection attacks • System and application vulnerabilities • Data locations and Regulation boundaries	• Firewall • Database • Application • IDS and IPS • Active Directory • Cloud system	• Connection logs, IPS and IDS logs, user logs: High • Database logs: Medium • Application logs: Low • System logs: High	• Proprietary APIs for each Cloud vendor complicate retrieval of evidence • Transient nature of data prevents verification of findings • Intruders can potentially target containers which service logging infrastructure

This study aims to identify smart city potential security, data privacy threats and provide recommendation and best practices based on study.

Literature Review

Adel S. Elmaghraby, Michael M. Losaviowritten in Journal of Advance Research (University of Cairo) under topic **"Cyber security challenges in Smart Cities: Safety, security and privacy"**[6]that Matching the security vulnerabilities Smarts City security may presented to unwitting users if clear theory of law and right defined what should be done with systems represented. It also mentioned the Jones GPS tracking case and suggested that a reevaluation of the concept of data privacy and third-party data collection should be undertaken in new age of electronic data collection and analysis.

Lei Cui, Gang Xie, Youyang Qu, Longxiang Gaoand Yunyun Yang mentioned in **"Security and Privacy in Smart Cities: Challenges and Opportunities"**[5]that use of smart application has caused many security and privacy issues. There is need of more robust and advance framework and protection models in academics and industry. There is strong need to satisfy the multiple security requirements of the rapidly developing smart applications to smarts cities and mitigation and presentation will be primary task in coming years of smart city studies.

Martin Dodge and Rob Kitchin wrote in**"The (in)security of smart cities: vulnerabilities, risks, mitigation and prevention"**[2]that smart city technologies are promoted as an effective way to manage and counter uncertainty and risk present in present day cities, but they also create new risks and make city insecure, criminal exploitation and disruption. There are five main vulnerabilities (weak software security and data encryption, use of insecure legacy systems and poor maintenance, large, complex and diverse, with many interdependencies and

large and complex attack surfaces, The interdependencies between smart city technologies and systems have the potential to create cascade effects, wherein 'highly interconnected entities rapidly transmit adverse consequences to each other' and vulnerabilities arising from human error and deliberate malfeasance of disgruntled (ex)employees) mentioned in the article.

Anwaar AlDairi and Lo'ai Tawalbeh suggested in**Cyber Security Attacks on Smart Cities and Associated Mobile Technologies** that cyber security is mainly affected by the emergent integration of technologies and resulted intensive communication, high interdependency and high complexity. This may lead to cryptography and unbound attack surface.

Zubair A. Baig, Patryk Szewczyk, Craig Valli, Priya Rabadia, Peter Hannay, Maxim Chernyshev, Mike Johnstone, Paresh Kerai, Ahmed Ibrahim, Krishnun Sansurooah, Naeem Syed, Matthew Peacock mentioned suggested in **Future challenges for smart cities: Cyber-security and digital forensics** thatchallenges associated with storage and acquisition of data related to smart city emerging from its components (UAV, BAS,Smart vehicle, cloud platform and IoT sensors).

Bako Ali and Ali Ismail Awad in **Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes [9]**usedOCTAVE allegro[10]to identified to 15 thread for smart home. The same model can extend to cover other smart city components.

Objective

The main objectives of research

1. Identify various factors, which influence overall security and data privacy of smart city.
2. Provide recommendations and best practices based on analysis.

Significance of research

1. This research will help in securing smart cities.

Research Methodology

The idea behind this research is to identify all factors which affects overall security and privacy of smart city.

Researcher will split overall research activity as below

1. Research area/locale
2. Research plan
3. Research design
4. Data collection method/technique
5. Data analysis
6. Implementation, conclusion and Summary

Research Area/Locale:

I have decided to choose Mahindra World City-Jaipur as locale for conducting research. The reasons for choosing Mahindra World City-Jaipur as below

1. First smart city developed by private sector.

2. It's world largest project to receive the coveted Stage 2 Climate Positive Development certification from the C40 Cities Climate Leadership Group.

3. The researcher based out of Delhi NCR and Jaipur is nearby hence most suitable for conducting research in cost effective and in a time bound manner.

Research Plan:

The research will be conduct in 4 phases

1. Phase I
    a. Formulating research problem by study security issues in smart cities.
    b. Detailing out research objectives and Conduct E2E process study

2. Phase II
    a. Preparing the research design
    b. Analysis

3. Phase III
    a. Result analysis and interpretation

4. Phase IV
    a. Report preparation andPresentation of results

5. Research Design:

The aim behind this study is to identify factors, which affects security and privacy of individual and systems for smart city. This study is exploratory in nature. The data received by studying facts will be arrange in tabular format. The analysis to be performed with the help of software tools to and drive conclusions.

References

[1] Smart City, https://en.wikipedia.org/wiki/Smart_city

[2] The (in)security of smart cities: vulnerabilities, risks, mitigation and prevention, Rob Kitchin and Martin Dodge

[3] https://internetofthingsagenda.techtarget.com/definition/smart-city

[4] IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey, Muhammad Burhan, Rana Asif Rehman, Bilal Khan and Byung-Seo Kim,https://www.mdpi.com/1424-8220/18/9/2796/htm

[5] Security and Privacy in Smart Cities:Challenges and Opportunities, Lei Cui, Gang Xie, Youyang Qu,Longxiang Gao AND Yunyun Yang.

[6] Cyber security challenges in Smart Cities: Safety, security and privacy by Adel S. Elmaghraby, Michael M. Losavio, https://www.sciencedirect.com/science/article/pii/S2090123214000290

[7] Cyber Security Attacks on Smart Cities and Associated Mobile Technologies, Anwaar AlDairi and Lo'ai Tawalbeh

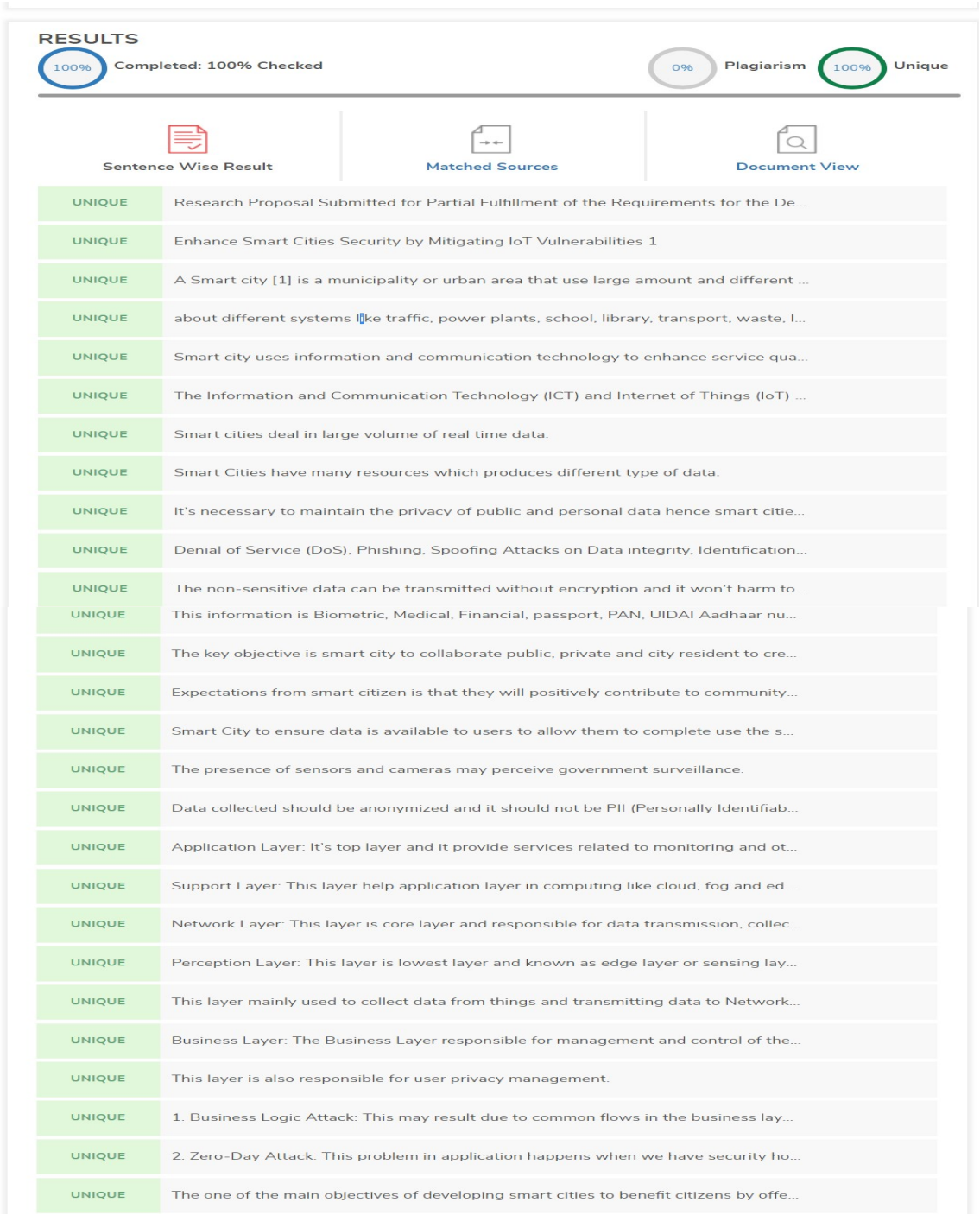
[8] Future challenges for smart cities: Cyber-security and digital forensics, Zubair A. Baig, Priya Rabadia, Patryk Szewczyk, Peter Hannay,Craig Valli,Maxim Chernyshev, Paresh Kerai, Mike Johnstone, Ahmed Ibrahim, Krishnun Sansurooah,Naeem Syed, Matthew Peacock.

[9] Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes, Bako Ali and Ali Ismail Awad

[10] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson

Plagiarism Checker Report

I have used http://smallseotools.com/plagiarism-checker/ to check.



RESULTS

100% Completed: 100% Checked

0% Plagiarism 100% Unique

Sentence Wise Result | Matched Sources | Document View

UNIQUE	Research Proposal Submitted for Partial Fulfillment of the Requirements for the De...
UNIQUE	Enhance Smart Cities Security by Mitigating IoT Vulnerabilities 1
UNIQUE	A Smart city [1] is a municipality or urban area that use large amount and different ...
UNIQUE	about different systems like traffic, power plants, school, library, transport, waste, l...
UNIQUE	Smart city uses information and communication technology to enhance service qua...
UNIQUE	The Information and Communication Technology (ICT) and Internet of Things (IoT) ...
UNIQUE	Smart cities deal in large volume of real time data.
UNIQUE	Smart Cities have many resources which produces different type of data.
UNIQUE	It's necessary to maintain the privacy of public and personal data hence smart citie...
UNIQUE	Denial of Service (DoS), Phishing, Spoofing Attacks on Data integrity, Identification...
UNIQUE	The non-sensitive data can be transmitted without encryption and it won't harm to...
UNIQUE	This information is Biometric, Medical, Financial, passport, PAN, UIDAI Aadhaar nu...
UNIQUE	The key objective is smart city to collaborate public, private and city resident to cre...
UNIQUE	Expectations from smart citizen is that they will positively contribute to community...
UNIQUE	Smart City to ensure data is available to users to allow them to complete use the s...
UNIQUE	The presence of sensors and cameras may perceive government surveillance.
UNIQUE	Data collected should be anonymized and it should not be PII (Personally Identifiab...
UNIQUE	Application Layer: It's top layer and it provide services related to monitoring and ot...
UNIQUE	Support Layer: This layer help application layer in computing like cloud, fog and ed...
UNIQUE	Network Layer: This layer is core layer and responsible for data transmission, collec...
UNIQUE	Perception Layer: This layer is lowest layer and known as edge layer or sensing lay...
UNIQUE	This layer mainly used to collect data from things and transmitting data to Network...
UNIQUE	Business Layer: The Business Layer responsible for management and control of the...
UNIQUE	This layer is also responsible for user privacy management.
UNIQUE	1. Business Logic Attack: This may result due to common flows in the business lay...
UNIQUE	2. Zero-Day Attack: This problem in application happens when we have security ho...
UNIQUE	The one of the main objectives of developing smart cities to benefit citizens by offe...

UNIQUE	We have below main applications in Smart Cities. [5]
UNIQUE	The key purpose of smart government to serve its citizen with infrastructure, data, ...
UNIQUE	This application helps in finding transportation facility, identify fast routes, vehicle ...
UNIQUE	This application helps in reducing waste, water, light, gas and thus help in protecti...
UNIQUE	This application provides medical facility to citizen, monitor health parameters, soci...
UNIQUE	This application helps in monitoring air quality, waste management efficiency, predi...
UNIQUE	We have above current technologies for handling data and privacy security threats ...
UNIQUE	This study aims to identify smart city potential security, data privacy threats and pr...
UNIQUE	Losavio written in Journal of Advance Research (University of Cairo) under topic "C...
UNIQUE	City security may presented to unwitting users if clear theory of law and right defin...
UNIQUE	It also mentioned the Jones GPS tracking case and suggested that a reevaluation o...
UNIQUE	Lei Cui, Gang Xie, Youyang Qu, Longxiang Gao and Yunyun Yang mentioned in "Sec...
UNIQUE	There is need of more robust and advance framework and protection models in aca...
UNIQUE	There is strong need to satisfy the multiple security requirements of the rapidly dev...

Share Report | Download Report | Start New Search

RESULTS

100% **Completed: 100% Checked**

0% **Plagiarism** 100% **Unique**

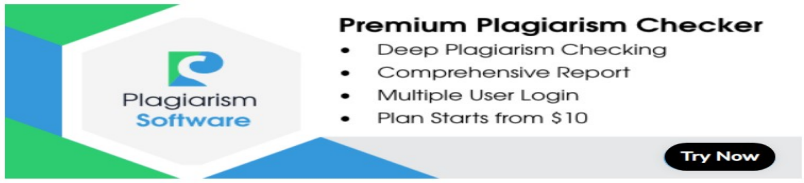
Sentence Wise Result | Matched Sources | Document View

UNIQUE	Martin Dodge and Rob Kitchin wrote in "The (in)security of smart cities: vulnerabilit...
UNIQUE	and counter uncertainty and risk present in present day cities, but they also create ...
UNIQUE	There are five main vulnerabilities (weak software security and data encryption, us...
UNIQUE	complex attack surfaces, The interdependencies between smart city technologies a...
UNIQUE	vulnerabilities arising from human error and deliberate malfeasance of disgruntled (...
UNIQUE	Anwaar AlDairi and Lo'ai Tawalbeh suggested in Cyber Security Attacks on Smart ...
UNIQUE	This may lead to cryptography and unbound attack surface.
UNIQUE	Baig, Patryk Szewczyk, Craig Valli, Priya Rabadia, Peter Hannay, Maxim Chernyshe...
UNIQUE	smart cities: Cyber-security and digital forensics that challenges associated with st...
UNIQUE	Bako Ali and Ali Ismail Awad in Cyber and Physical Security Vulnerability Assessm...
UNIQUE	The same model can extend to cover other smart city components.

UNIQUE	1. Identify various factors, which influence overall security and data privacy of sma...
UNIQUE	2. Provide recommendations and best practices based on analysis.
UNIQUE	1. This research will help in securing smart cities.
UNIQUE	The idea behind this research is to identify all factors which affects overall security ...
UNIQUE	I have decided to choose Mahindra World City-Jaipur as locale for conducting resea...
UNIQUE	The reasons for choosing Mahindra World City-Jaipur as below
UNIQUE	2. It's world largest project to receive the coveted Stage 2 Climate Positive Develop...
UNIQUE	3. The researcher based out of Delhi NCR and Jaipur is nearby hence most suitable ...
UNIQUE	a. Formulating research problem by study security issues in smart cities.
UNIQUE	b. Detailing out research objectives and Conduct E2E process study
UNIQUE	The aim behind this study is to identify factors, which affects security and privacy ...
UNIQUE	The data received by studying facts will be arrange in tabular format.
UNIQUE	The analysis to be performed with the help of software tools to and drive conclusio...
UNIQUE	[2] The (in)security of smart cities: vulnerabilities, risks, mitigation and prevention, ...
UNIQUE	[4] IoT Elements, Layered Architectures and Security Issues: A Comprehensive Sur...
UNIQUE	[5] Security and Privacy in Smart Cities: Challenges and Opportunities, Lei Cui, Ga...
UNIQUE	[6] Cyber security challenges in Smart Cities: Safety, security and privacy by Adel S.
UNIQUE	[7] Cyber Security Attacks on Smart Cities and Associated Mobile Technologies, A...
UNIQUE	[8] Future challenges for smart cities: Cyber-security and digital forensics, Zubair A.
UNIQUE	Baig, Priya Rabadia, Patryk Szewczyk, Peter Hannay, Craig Valli, Maxim Chernyshe...
UNIQUE	[9] Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Ho...
UNIQUE	[10] Introducing OCTAVE Allegro: Improving the Information Security Risk Assess...

Share Report | Download Report | Start New Search

YOUR PRIVACY,OUR PRIORITY
Small seo tools are specially designed to automatically delete any record of search/check made on them.



Plagiarism Checker API | Plagiarism Checker WP Plugin

SPONSORED SEARCHES
CHECK MY GRAMMAR | TESTING SOFTWARE